Najnovšie post-kvantové štandardy v kryptografii

Vladyslav Lanovyi

Obsah

Zoznam skratiek

AES - Advanced Encryption Standard
DES - Data Encryption Standard
RSA - Rivest-Shamir-Adleman
ECC - Elliptic Curve Cryptography
ECDSA - Elliptic Curve Digital Signature Algorithm
SHA - Secure Hash Algorithm
NTT - Number Theoric Transform

Úvod

1 Chronológia vývoja kryptografických štandardov

1.1 Symetrické štandardy

1.1.1 DES (Data Encryption Standard)

1.1.2 AES (Advanced Encryption Standard)

1.2 Štandardizácia verejno-kľúčovej kryptografie

1.2.1 DSS (Digital Signature Standard)

1.3 Hašovacie štandardy

1.3.1 SHS (Secure Hash Standards)

2 Kvantova a post-kvantova kryptografia

2.1 Kvantova kryptografia

2.2 Postkvantova kryptografia

3 NIST štandarty pre post-kvantovú kryptografiu

3.1 FIPS-203 (CRYSTALS-Kyber)

3.1.1 Zakladne pojmy a opis

3.2 FIPS-204 (CRYSTALS-Dilithium)

3.2.1 Zakladne pojmy a opis

3.3 FIPS-205 (SPINCS+)

3.3.1 Zakladne pojmy a opis

4 Experimentálna časť

5 Záver

Literatúra